UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,683	12/08/2003	Joon-Kit Goh	SI-0039	5707

29293 1590 04/03/2008
ESCHWEILER & ASSOCIATES, LLC
NATIONAL CITY BANK BUILDING
629 EUCLID AVE., SUITE 1000
CLEVELAND, OH 44114

EXAMINER	
PATEL, NIRAV B	
ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
04/04/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing@eschweilerlaw.com

Respond to OA
3mo. 7.4.08
6mo. 10.4.08

DOCKETED

RECEIVED
APR 16 2008
BY:

Office Action Summary	Application No.	Applicant(s)	
	10/730,881	GOH, JOON-KIT	
	Examiner	Art Unit	
	NIRAV PATEL	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-32 and 34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-32, 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *9/19/07, 1/10/08*.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

1. Applicant's amendment filed on Jan. 07, 2008 has been entered. Claims 1, 3-32, 34 are pending. Claims 1, 3, 10, 11, 12, 19, 20, 30 are amended and Claims 2, 33 are cancelled by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made

2. Claims 1, 3, 4, 6, 9-21, 23, 26-32, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qi et al (US Patent No. 7,142,671) and in view of Anand (US Patent No. 7,280,657).

As per claim 1, Qi teaches: the DES engine having a message input, a cipher key input, and a pre-data output, the engine adapted to receive and selectively process a block of data from the message input of the security processing circuit during a first DES processing operation, and subsequently to process data from an intermediate result during second and third DES processing operations and store an intermediate result of the third DES processing operation to the pre-data output [Fig. 4A, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-14]; a security keys circuit having a set of cipher keys input and a key output, the security keys circuit operable to select and transfer a different cipher key to the key output coupled to the cipher key input of the DES engine selected from the set of cipher keys associated with each DES processing operation during the first, second and third DES processing operations [Fig. 4A – 419 col. 8 lines 29-64]; and a data output circuit having a pre-data input and a data output, the pre-data input of the data output circuit coupled to the pre-data output of the DES engine, and the data output selectively

coupleable to the host system, the data output circuit operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A, 1, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-14], wherein the DES engine comprises: a permutation block having the message input and a permutation output, the permutation block operable to receive a block of data at the message input and to perform an initial permutation of the message input data and provide a permutation result at the permutation output [Fig. 4A, 4B, 5, col. 7 lines 6-29, col. 9 lines 15-19]; a data input multiplexer having a first and second input and a data selection output, the data input multiplexer operable to select and couple one of the first and second inputs to the data selection output; an intermediate result register having a data input, a clock input, and a latched data output, the register operable to store right and left half results of the initial permutation or of a cipher process based on data present at the data input upon receipt of a clock signal at the clock input; a pre-data output multiplexer having a first and second input and a data selection output, the pre-data output multiplexer operable to select and couple one of the first and second inputs to the data selection output [Fig. 4A,4B]; and a pre-data output register having a data input, a clock input, and a latched data output [Fig. 4A, 4B], wherein the permutation output of the permutation block is coupled to the first input of the data input multiplexer, the data selection output of the data input multiplexer coupled to the data input of the intermediate result register, the latched data output of the intermediate result register coupled to the data input of the cipher blocks having the cipher output of the cipher blocks feedback coupled to the second input of the data input multiplexer and to the first input of the pre-data output multiplexer the data selection output of the pre-data output multiplexer coupled to the pre-data output register, the latched data output of the pre-data output

register feedback coupled to the second input of the pre-data output multiplexer and the pre-data output [Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32].

Qi teaches cipher block for performing the ciphering process and providing the result to the intermediate register as above.

Anand teaches: eight cipher blocks having a data input, a key input, and a cipher output, operable to receive data at the data input and a key at the key input, to perform the cipher process comprising right and left halves of cipher process on the data at the data input employing the key, and to provide a first and second cipher result cycle of each of the three DES processing operations [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Anand with Qi, since one would have been motivated to increase the security or to make a cipher stronger and perform the encryption and decryption in less time [Anand, col.2 lines 3-5, 35-41].

As per claim 3, the rejection of claim 2 is incorporated and Qi discloses:

wherein the DES engine is further operable to perform the initial permutation of the message input data using the permutation block, initially select the permutation result with the data input multiplexer and couple and store the result to the intermediate result register during a data input latch cycle, to transfer the initial result and the cipher key from the security keys circuit to the cipher blocks for cipher processing and intermediate storage of the right and left halves of the first step cipher results subsequent to selection of the second input of the data input multiplexer into the intermediate result register during the first cipher process cycle, to transfer the stored intermediate result and the cipher key from the security keys circuit to the cipher blocks for cipher

processing and intermediate storage of the right and left halves of the second step cipher results subsequent to selection of the second input of the data input multiplexer into the intermediate result register and the pre-data output register subsequent to selection of the first input of the pre-data output multiplexer during the second cipher process cycle of the first DES processing operation, and wherein the DES engine is operable to repeat the first and second cipher process cycles for the subsequent second and third DES security processing operations of the security processing circuit [Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32], and latch the intermediate result of the third DES operation to the pre-data output of the pre-data output register of the DES engine, using the selection of the second input of the pre-data output multiplexer during the third DES processing operation of the 3DES security processing [Fig. 4A, 4B, col. 8 lines 44-67-col. 9 lines 1-14].

Anand teaches eight cipher blocks for cipher processing [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

As per claim 4, the rejection of claim 3 is incorporated and Qi discloses: wherein the 3DES processing is completed in three single DES processing operations [col. 5 lines 35-42, col. 8 lines 65-67].

As per claim 6, the rejection of claim 3 is incorporated and Anand discloses: Wherein the first, second and third DES processing operations each have a duration of two clock cycles [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

As per claim 9, the rejection of claim 1 is incorporated and Qi discloses: coupled to one or more of the DES engine, the security keys circuit, and the data output circuit for timing clock cycles of the first, second and third DES processing operations of the 3DES processing for the security processing circuit [Fig. 4A, 4B, 5].

As per claim 10, the rejection of claim 1 is incorporated and Qi discloses:

a set of cipher keys input, wherein the set of cipher keys comprise three different cipher keys, each cipher key associated with one of the three DES processing operations of the 3DES security processing [Fig. 4A]; a keys input multiplexer having a set of cipher keys input, and a cipher key selection output, the keys input multiplexer operable to select and couple a cipher key to the cipher key selection output [Fig. 4A]; and a security keys register having a data input, a clock input, and a latched data output, the register operable to store the cipher key selection associated with one of the three DES processing operations of the 3DES security processing based on cipher key data at the data input upon receipt of a clock signal at the clock input, the latched data output of the security keys register coupled to the key input of the cipher blocks [Fig. 4A, col. 8 lines 29-67, col. 9 lines 1-14]. Anand teaches the eight cipher blocks [Fig. 2A].

As per claim 11, the rejection of claim 10 is incorporated and Qi discloses: the keys input multiplexer is operable to receive the three cipher keys and to selectively couple one of the three cipher keys associated with a DES processing operation to the DES engine during the three DES processing operations of the 3DES security process [Fig. 4A].

As per claim 12, the rejection of claim 1 is incorporated and Qi discloses: an inverse permutation block IPB having a pre-data input and an inverse permutation output, the block operable to receive and further security process the pre-data output from the DES engine, performing an inverse permutation of the pre-data and transfer the processed data to the inverse permutation output [Fig. 4A, col. 9 lines 58-67, col. 10 lines 1-14]; an XOR gate XOR having a processed data input, an initialization vector input, and an XOR gate output, the XOR gate operable to selectively exclusive OR the initialization vector at the initialization vector input together with the processed data from the inverse permutation output of the inverse permutation block coupled to the processed data

input, and transfer the XOR data to the XOR gate output [Fig. 4A, 4B, col. 8 lines 44-64]; a data output multiplexer having a first and second input, a selection control signal, and a data selection output, the data output multiplexer operable to select and couple one of the first and second inputs to the data selection output, based on the state of the selection control signal, the first input coupled to the XOR gate output, and the second input coupled to a data output register [Fig. 4A, 4B]; and the data output register having a data input, a clock input, and a latched data output, the register operable to store the output data results of the third DES process based on data present at the data input upon receipt of a clock Signal at the clock input, the latched data output of the data output register feedback coupled to the second input of the data output multiplexer to insure latching of the data at the output, wherein the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A, 4B, 5, col. 8 lines 44-67, col. 9 lines 1-14].

As per claim 13, the rejection of claim 12 is incorporated and Qi discloses: the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A].

As per claim 14, the rejection of claim 1 is incorporated and Qi discloses: wherein the security processing circuit resides within a network interface device of a host system for performing 3DES encryption and decryption services for the host system using a DES engine [Fig. 1, 4A, col. 3 lines 39-57].

As per claim 15, the rejection of claim 1 is incorporated and Qi discloses: a network interface device coupled with the security processing circuit, the network interface device being adapted to selectively

encrypt outgoing data from the host system to cryptographically process data for transmission to the network [Fig. 1, 4A, 4B].

As per claim 16, the rejection of claim 15 is incorporated and Qi discloses: the network interface device comprises a bus interface, a media access control system, and the security processing circuit [Fig. 1].

As per claim 17, the rejection of claim 16 is incorporated and Qi discloses: the network interface device is a single integrated circuit [Fig. 1].

As per claim 18, the rejection of claim 1 is incorporated and Qi discloses: the circuit comprises an IPsec circuit adapted to selectively provide authentication, encryption, and decryption functions for incoming and outgoing data [Fig. 1, 2].

As per claim 19, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 20, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

As per claim 21, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 23, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 26, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 9. Thus, it is rejected with the same rationale applied against claim 9 above.

As per claim 27, Qi discloses: selecting a permutation result of the initial permutation to couple the result to an intermediate result register during a first DES process; storing the permutation result in the intermediate

result register [Fig. 4A col. 7 lines 12-61]; cipher processing the stored permutation result using an cipher block to generate an intermediate result of the cipher processing; selectively storing the intermediate result in the intermediate result register [Fig. 4A, 4B, 5, col. 8 lines 10-53]; cipher processing the stored intermediate result using the cipher blocks to generate a first DES result of the cipher processing [Fig. 4A, 4B col. 8 lines 44-67, col. 9 lines 1-14]; and selectively storing the first DES result in the intermediate result register [Fig. 4A, 4B]. Qi teaches cipher block for performing the ciphering process and providing/storing the result to the intermediate register as above.

Anand teaches: eight cipher blocks to generate an intermediate result of the ciphering processing; ciphering processing the stored intermediate result using the eight cipher blocks to generate the DES result of the cipher processing [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Anand with Qi, since one would have been motivated to increase the security or to make a cipher stronger and perform the encryption and decryption in less time [Anand, col.2 lines 3-5, 35-41].

As per claim 28, the rejection of claim 27 is incorporated and Qi discloses: wherein a second DES process further comprises: cipher processing the stored first DES result using the cipher blocks to generate a second intermediate result of the cipher processing [Fig. 4A, 4B, col. 8 lines 29-43]; selectively storing the second intermediate result in the intermediate result register [Fig. 4A, 4B]; cipher processing the stored second intermediate result using the cipher blocks to generate a second DES result of the cipher processing [Fig. 4A, 4B, col. 8 lines 29-43]; and selectively storing the second DES result in the intermediate result register [Fig. 4A, 4B, 5, col. 8 lines 44-67, col. 9 lines 1-14].

Anand teaches: a second DES process further comprises: eight cipher blocks to generate an intermediate result of the ciphering processing; ciphering processing the stored intermediate result using the eight

cipher blocks to generate the DES result of the cipher processing [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

As per claim 29, the rejection of claim 28 is incorporated and Qi discloses:

cipher processing the stored second DES result using the cipher blocks to generate a third intermediate result of the cipher processing [Fig. 4A, 4B, col. 8 lines 29-67, col. 9 liens 1-14]; selectively storing the third intermediate result in the intermediate result register [Fig. 4A]; cipher processing the stored third intermediate result using the cipher blocks to generate a third pre-data DES result of the cipher processing [Fig. 4A, 4B, col. 8 lines 44-67]; selectively storing the third pre-data DES result in the intermediate result register and selectively storing the third pre-data DES result in a pre-data output register [Fig. 4A, col. 8 lines 44-67]; performing an inverse permutation of the third pre-data DES result [Fig. 4A, col. 9 lines 34-65]; exclusively ORing the result of the inverse permutation with an initialization vector to generate a 3DES result [Fig. 4A, col. 8 lines 57-64]; and selectively latching the 3DES result to a data output register [Fig. 4A].

Anand teaches: a third DES process further comprises: eight cipher blocks to generate an intermediate result of the ciphering processing; ciphering processing the stored intermediate result using the eight cipher blocks to generate the DES result of the cipher processing [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

As per claim 30, Qi discloses:

receiving data of a permutation result of the initial permutation to a data input multiplexer during a first DES process [Fig. 4A col. 7 lines 12-61, 4B]; selecting and coupling the permutation result at the data input multiplexer to an intermediate result register; storing the permutation result in the intermediate result register[Fig. 4A, 4B];

transferring the stored permutation result and a cipher key to an cipher blocks for cipher processing; cipher processing using the cipher blocks to generate data of an intermediate result of the cipher processing [Fig. 4A, 4B, 5, col. 8 lines 10-53]; storing the intermediate result in the intermediate result register [Fig. 4A, 4B]; transferring the stored intermediate result and the cipher key to the cipher blocks for cipher processing [Fig. 4A, 4B]; cipher processing the intermediate result data using the cipher blocks to generate a first DES result of the cipher processing [Fig. 4A, 4B]; and storing the first DES result in the intermediate result register [Fig. 4A, 4B].

Anand teaches: a DES process further comprises: eight cipher blocks for ciphering processing; ciphering processing using the eight cipher blocks [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Anand with Qi, since one would have been motivated to increase the security or to make a cipher stronger and perform the encryption and decryption in less time [Anand, col.2 lines 3-5, 35-41].

As per claim 31, the rejection of claim 30 is incorporated and it encompasses limitations that are similar to limitations of claim 28. Thus, it is rejected with the same rationale applied against claim 28 above.

As per claim 32, the rejection of claim 31 is incorporated and it encompasses limitations that are similar to limitations of claim 29. Thus, it is rejected with the same rationale applied against claim 29 above.

As per claim 34, it encompasses limitations that are similar to limitations of claim 30. Thus, it is rejected with the same rationale applied against claim 30 above. Further, Anand teaches transferring the first intermediate result data from the register to a set of eight ciphering block for ciphering processing during a first cycle of the DES processing; DES processing the data using the set of eight cipher blocks to produce a second intermediate result; transferring the second intermediate result data from the register to the set of eight cipher blocks for cipher processing during a second cycle of the DES processing; storing the

intermediate result back in the intermediate result register on the second cycle of the DES processing [Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25].

3. Claims 5, 7, 8, 22, 24, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qi et al (US Patent No. 7,142,671) in view of Anand (US Patent No. 7,280,657) and in view of Callum (US Patent No. 6,985,581).

As per claim 5, the rejection of claim 3 is incorporated and Callum discloses:

wherein the 3DES processing is completed in eight clock cycles [Fig. 3 col. 2 lines 46-67, col. 3 lines 1-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Callum with Qi and Anand, since one would have been motivated to increase the security or to make a cipher stronger and perform the encryption and decryption in less time [Anand, col.2 lines 3-5, 35-41].

As per claim 7, the rejection of claim 3 is incorporated and Callum discloses: the clock cycle has a period of about 8ns [Fig. 3].

As per claim 8, the rejection of claim 5 is incorporated and Callum discloses: wherein the eight clock cycle of the 3DES security processing comprise: a data input latch cycle; a first DES processing operation comprising two cycles; a second DES processing operation comprising two cycles; a third DES processing operation comprising two cycles; and a data output latch cycle [Fig. 3 col. 2 lines 46-67, col. 3 lines 1-25].

As per claim 22, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 24, the rejection of claim 22 is incorporated and it encompasses limitations that are similar to limitations of claim 7. Thus, it is rejected with the same rationale applied against claim 7 above.

As per claim 25, the rejection of claim 22 is incorporated and it encompasses limitations that are similar to limitations of claim 8. Thus, it is rejected with the same rationale applied against claim 8 above.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 4-9, 11, 13-18, 27-30, 32, 34 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6, 11-18, 23-28 of copending application no. 10/730640. Although the conflicting claims are not identical, they are not patentably distinct from the pending claim and as such are unpatentable for obvious-type double patenting.

The copending application 10/730640 ('640): Claims 1-6, 11-18, 23-28 recite, "A security processing circuit for performing 3DES encryption or decryption service using a single DES engine, the security processing circuit comprising: the single DES engine operable to provide security processing,.....; a select switch coupled to the data input of the security processing circuit.....; a set of cipher keys selectively coupled to the single DES engine, wherein the security processing circuit is operable to select

and load a different cipher key associated with each DES processing operation to the single DES engine during the three single DES processing operations of the 3DES security processing; and a clock input coupled to the single DES engine for timing clock cycles of the first, second and third single DES processing operations, wherein the 3DES processing is completing in eight clock cycles, or wherein in the first, second and third DES processing operations have a during comprising two clock cycles each, wherein the select switch (multiplexer) is operable to selectively couple one of the data input and the intermediate result to the single DES engine according to the state of a selection signal coupled to the select switch; wherein the set of cipher keys comprise three different cipher keys, each cipher key associated with one of the three DES processing operations of the 3DES security processing; wherein the clock cycle has a period of about 8ns; wherein the eight clock cycles of the 3DES security processing comprise: a data input latch cycle; a first DES processing operation comprising two cycles; a second DES processing operation comprising two cycles; a third DES processing operation comprising two cycles; and a data output latch cycle; wherein the security processing circuit reside within a network interface device of a host system for performing 3DES encryption and decryption services for the host system using a single DES engine; further a network interface device coupled with the security processing circuit, the network interface device being adapted to selectively encrypt outgoing data from a host system to cryptographically process data for transmission to a network.

Claims 1, 4-9, 11, 13-18, 27-30, 32, 34 of the instant application are obvious over claims 1-6, 11-18, 23-28 above, as they performing 3DES IPsec security processing service for a host system using a DES engine. It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize a single DES engine for providing gigabit/s IPsec security processing within a host network interface (Appl. # '640, page 1 lines 10-12).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Response to Argument

4. Applicant's arguments filed Jan. 07, 2008 have been fully considered. In view of applicant's argument that Qi does not teach or suggest "eight cipher blocks or eight round ciphering processes", is found persuasive. Newly found reference by Anand teaches the triple DES processing using the eight cipher blocks process (Fig. 1, 2A, 2B, col. 3 lines 32-52, col. 4 lines 3-25) and is used with the previously cited references. See detail action above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Averbuj et al (US 7212631) – Apparatus and method for performing Kasumi ciphering

McCanny et al (US 2003/0053623) – Apparatus for selectably encrypting or decrypting data

Matsui et al (US 2002/0159599) --- Block encryption device using auxiliary conversion

Lim (US 2002/0003876) – Encryption apparatus using data encryption standard algorithm.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NP
3/24/08
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135

Notice of References Cited	Application/Control No. 10/730,681	Applicant(s)/Patent Under Reexamination GOH, JOON-KIT	
	Examiner NIRAV PATEL	Art Unit 2135	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,280,657	10-2007	Anand, Satish N.	380/37
*	B	US-6,995,581	01-2006	Callum, Roy	380/2
*	C	US-7,212,631	05-2007	Avanbuj et al.	380/37
*	D	US-2002/0003876	01-2002	Lim, Young-Won	380/29
*	E	US-6,324,286	11-2001	Lai et al.	380/29
*	F	US-2002/0159589	10-2002	Matsui et al.	380/263
*	G	US-2003/0053823	03-2003	McGenny et al.	380/37
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.